GANPAT UNIVERSITY									
FACULTY OF ENGINEERING AND TECHNOLOGY									
Programme	Bachelor of Technology					Branch/Spec.	Computer Science & Engineering (CBA)		
Semester	VII					Version	1.0.0.0		
Effective from Academic Year			2022-23			Effective for the batch Admitted in			June 2019
Subject code	2CSE709		Subject Name			Cloud Security			
Teaching scheme						Examination scheme (Marks)			
(Per week)	Lecture(DT)		Practical(Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	3	0	2	0	5	Theory	40	60	100
Hours	3	0	4	0	7	Practical	60	40	100

Pre-requisites:

Cloud Foundations, LINUX, Programming and Database, Information Security

Learning Outcome:

After completion of the course, student will be able to:

- Understand the cloud security for infrastructure and applications.
- Understand the concepts of private and public clouds using modern approaches and tools.
- Design security models for various business scenarios.
- Implement and Deploy lightweight Security Services.

Theory syllabus

Unit	Content	Hrs
1	**Cloud Security Fundamentals** Introduction to Cloud Security, Basic concepts (CIA) - Confidentiality, Integrity and Availability, Understanding Multi tenancy, Multi tenancy concepts, Design considerations for multi-tenant cloud, Security concerns on multi-tenant cloud environments, Security in context of Cloud Deployment and consumption models, Cloud Governance, Risk and Compliance	**12**
2	**Virtualization and Container Security** Virtualization Security, Vulnerabilities in management, Vulnerabilities in Hypervisor, Vulnerabilities in Virtualization and virtual machines, Platform Hardening to Prevent Threats, Container Security, Network isolation and Protection , Setting up a secure network, Network isolation and segmentation, Load balancer and Ingress services	**8**
3	**Identity and Access Management (IAM)** Identity and Access Management (IAM), IAM Operational Areas, Cloud Identity Management, Identity Provisioning in Cloud, Cloud Authentication, SAML, OAuth2.0, OpenID, Multi Factor authentication, Enterprise SSO and federation, Privileged Access Management (PAM), IBM Cloud App ID	**9**
4	**Data Security** Data Security, protection and IBM key protect in IBM Cloud, Data Integrity in the Cloud, IBM Multi-Cloud Data Encryption, Data in Transit, Protect Data in Transit, Certificate management, Digital certificates Encrypting data in transit, Istio overview to protect microservices	**8**

5	**DevSecOps** Application Security, Secure DevOps, Vulnerability and Patch Management, IBM Cloud Pak for Security	**8**

Self learning: CASE studies

Practical content

Practicals will be based on topics like cloud deployment models,container security,Identity authentication and provisioning,data security, secure devOps.

Text Books

1	Enterprise Cloud Security and Governance: Efficiently Set Data Protection and Privacy Principles by Zeal Vora

Reference Books

1	Cloud Security: A Comprehensive Guide to Secure Cloud Computing 1st Edition, Kindle Edition
2	Cloud Security Automation: Get to grips with automating your cloud security on AWS and OpenStack

Course Outcomes:

COs	Description
CO1	Understand the cloud security for infrastructure and applications.
CO2	Understand the concepts of private and public clouds using modern approaches and tools.
CO3	Design security models for various business scenarios.
CO4	Implement and Deploy lightweight Security Services.

Mapping of CO and PO:

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	2	3	3	2	1	2	1	2	3	2
CO2	2	3	2	2	2	3	2	0	2	2	0	2
CO3	3	3	O	3	2	3	2	2	3	2	2	1
CO4	3	3	3	2	0	3	3	2	2	3	3	3